

Digit Polynomials and their application to integer factorization

Markus Hittmeir
University of Salzburg
Mathematics Department

Abstract

This paper presents the concept of *digit polynomials*, which leads to a deterministic and unconditional integer factorization algorithm with the runtime complexity $\mathcal{O}(N^{1/4+\epsilon})$. Strassen's well known factoring approach is a special case of our method. We will also consider a possibility to improve upon the complexity bound.

1 Introduction

We consider the problem of computing the prime factorization of a given natural number N . Currently, the best publicly known deterministic and unconditional factorization algorithms all have a runtime complexity of the form $\mathcal{O}(N^{1/4+\epsilon})$ [W, p.240]. A method which achieves this complexity is the approach of Strassen [S], based on the idea to compute parts of $\lfloor N^{1/2} \rfloor!$ to find a nontrivial factor of N . A recent improvement of the logarithmic factor in the complexity bound can be found in [CH]. For a general overview, the reader may consult [P].

In this paper we present a method based on products of certain polynomials. The main idea is to construct polynomials $g \in \mathbb{Z}[X]$ such that as many integers x , $0 \leq x \leq N-1$, as possible satisfy

$$1 < \gcd(g(x), N) < N.$$

Several b -adic representations of N are used in Theorem 2.9, which yields a method to construct such a polynomial of degree d with complexity $\mathcal{O}(d^{1+\epsilon})$.

The author is supported by the Austrian Science Fund (FWF): Project F5504-N26.
Address: Hellbrunnerstraße 34, A-5020 Salzburg. E-Mail: markus.hittmeir@sbg.ac.at
2010 *Mathematics Subject Classification*: Primary 11A51; Secondary 11A41.
Key words and phrases: Factorization, Primality, Primes.

In the factorization algorithm we will not only make use of the *cardinality*, but also of the *position* of those x with the property above.

Our deterministic method is not appropriate for factorizing large numbers. In practice, probabilistic algorithms with much lower complexity are used for this task (See [R] and [CP]).

2 Basic Ideas

Throughout this paper, \mathbb{P} denotes the set of primes. We call a natural number semiprime if and only if it is the product of two distinct primes. Let $n \in \mathbb{N}$. We denote the complete residue system $\{0, \dots, n-1\}$ modulo n by Z_n and the residue class ring $\mathbb{Z}/n\mathbb{Z}$ by \mathbb{Z}_n . For $f \in \mathbb{Z}[X]$, we write the leading coefficient of f as $\text{lc } f$. Until further notice, let $N \in \mathbb{N}$ be fixed.

Definition 2.1. Let $b \in \mathbb{Z}$. We denote the set of polynomials $f \in \mathbb{Z}[X]$ with the property $f(b) = N$ by $\mathcal{D}_{N,b}$. The elements of $\mathcal{D}_{N,b}$ are called *digit polynomials of N to base b* .

Definition 2.2. Let $b \in \mathbb{N}$, $b \geq 2$. Let $N = \sum_{i \geq 0} n_i b^i$ be the unique b -adic representation of N with digits $n_i \in \{0, \dots, b-1\}$. Define

$$P_b := \sum_{i \geq 0} n_i X^i \in \mathbb{Z}[X].$$

We call P_b the *b -adic digit polynomial of N* . Clearly, we have $P_b \in \mathcal{D}_{N,b}$.

Lemma 2.3. Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N,b}$. Then, for every $x \in \mathbb{Z}$, we have $N \equiv f(x) \pmod{x-b}$.

Proof. We know that b is a zero of the polynomial $f - N$, hence $X - b$ divides $f - N$ in $\mathbb{Z}[X]$ and the congruence holds for every evaluation. \square

Corollary 2.4. Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N,b}$. We conclude for every $x \in \mathbb{Z}$ that $\gcd(N, x-b) = \gcd(f(x), x-b)$, and that $x-b \mid N$ iff $x-b \mid f(x)$.

Lemma 2.5. Let u and v be nontrivial and coprime divisors of N . Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N,b}$ such that

1. $\gcd(\text{lc } f, N) = 1$ and
2. $d := \deg f$ is smaller than the largest prime factor of v .

Then there exists $x \in \mathbb{Z}$ with $u \mid f(x)$ and $v \nmid f(x)$.

Proof. Let $y \in \mathbb{Z}$ be arbitrary. Let $x \in \mathbb{Z}$ with $uy = x - b$. From Lemma 2.3 we derive $u \mid f(x)$, hence $u \mid f(uy + b)$ for any $y \in \mathbb{Z}$. We have to show that there exists $y \in \mathbb{Z}$ with $v \nmid f(uy + b)$.

Assume to the contrary that $f(uy + b) \equiv 0 \pmod{v}$ for all $y \in \mathbb{Z}$. Write $f(uy + b)$ as $f(b) + u \cdot g(y)$ for $g \in \mathbb{Z}[X]$. It is easy to verify that $\deg g = d$ and $\text{lc } g = u^{d-1} \text{lc } f$. Let p be the largest prime factor of v . Then, for every $y \in \mathbb{Z}$, it follows that

$$f(uy + b) = u \cdot g(y) + f(b) \equiv u \cdot g(y) \equiv 0 \pmod{p}.$$

The fact $p \nmid u$ implies $g(y) \equiv 0 \pmod{p}$ for every $y \in \mathbb{Z}$. But, since $\gcd(\text{lc } f, N) = 1$, we get $p \nmid \text{lc}(g)$. Therefore, g is of degree d in $\mathbb{Z}_p[X]$ and, for this reason, has at most d zeros in $\mathbb{Z}_p[X]$. From $d < p$ the contradiction follows. \square

In the proof of the preceding lemma we have seen that, if N is a composite number and if $f \in \mathcal{D}_{N,b}$ is chosen with appropriate degree, we get various integers $x \in Z_N$ such that $1 < \gcd(f(x), N) < N$.

Definition 2.6. Let $g \in \mathbb{Z}[X]$. An element $x \in Z_N$ is called *suitable for g* , if and only if $1 < \gcd(g(x), N) < N$. We also define

$$\nu(g) := \#\{x \in Z_N : x \text{ is suitable for } g\}.$$

If we multiply two polynomials $f, g \in \mathbb{Z}[X]$, it may happen that $x \in Z_N$ is suitable for f and for g , but not for $f \cdot g$.

Definition 2.7. Let $d \in \mathbb{N}$ and $f_i \in \mathbb{Z}[X]$, $1 \leq i \leq d$. An element $x \in Z_N$ *vanishes in $g := \prod_{i=1}^d f_i$* , if and only if $\gcd(g(x), N) = N$ and there is at least one i such that x is suitable for f_i .

Theorem 2.8. Let $N \in \mathbb{N}$ be a semiprime number with the prime factors p and q and assume $p < q$. Let $f \in \mathbb{Z}[X]$ and $d := \deg f$. Let n be the number of distinct zeros of f modulo p and m be the number of distinct zeros of f modulo q . Then:

1. $\nu(f) = mp + nq - 2nm$.
2. Let $f \neq 0$ in $\mathbb{Z}_p[X]$ and in $\mathbb{Z}_q[X]$. If $d < p/2$, then $\nu(f) \leq dp + dq - 2d^2$.

Proof. For 1: Let $x \in Z_N$ be suitable for f . Then x is a zero of f either modulo p or modulo q . Let $\alpha_1, \dots, \alpha_n$ be the distinct zeros of f modulo p and β_1, \dots, β_m be the distinct zeros of f modulo q . For $i = 1, \dots, n$ and $j = 1, \dots, m$ we consider

$$\begin{aligned} &py + \alpha_i, \text{ for } y = 0, \dots, q-1, \\ &qy + \beta_j, \text{ for } y = 0, \dots, p-1. \end{aligned}$$

Every x which is suitable for f is of that form, and these are a priori $mp+nq$ values in Z_N . But some of them might be equal. First, we show that the values of the form $py + \alpha_i$ are distinct modulo N . We assume that there are $y_1, y_2 \in Z_q$ with $py_1 + \alpha_i \equiv py_2 + \alpha_k \pmod{N}$ for some $i, k \in \{1, \dots, n\}$. For $i \neq k$ this is not possible, because we get $\alpha_i \equiv \alpha_k \pmod{p}$, which contradicts the assumption that the zeros are distinct modulo p . For $i = k$, it follows that $y_1 \equiv y_2 \pmod{q}$. Hence, the congruence only holds if we compare the value $py_1 + \alpha_i$ with itself. For this reason, all these values are distinct. By similar arguments, one can show that this also holds for the values of the form $qy + \beta_j$.

Next, we consider the case that some value of the form $py + \alpha_i$ is congruent to some value of the form $qy + \beta_j$. Then this value is a zero of f modulo N . By the Chinese Remainder Theorem, one can easily verify that f must have exactly nm distinct zeros modulo N . Since any zero z of f modulo N is also a zero of f modulo p and modulo q , we can write $z = py_1 + \alpha_i = qy_2 + \beta_j$ for some y_1, y_2 and i, j . Hence, at every zero of f modulo N exactly two equal values of our list above coincide. The other values all satisfy $1 < \gcd(f(x), N) < N$. Therefore, we get $\nu(f) = mp + nq - 2nm$.

For 2: Consider $h = -2XY + Xq + Yp \in \mathbb{Z}[X, Y]$. Since f has at most d distinct zeros modulo p and modulo q , we want to maximize this function for $(x, y) \in [0, d]^2$. We get

$$h_X(x, y) = -2y + q \text{ and } h_Y(x, y) = -2x + p$$

as partial derivatives. Hence, the only critical point is $(x, y) = (p/2, q/2)$. But this point is not in $[0, d]^2$, so we consider h on the boundary and get $g_1(x) = xq$, $g_2(x) = xp$, $g_3(x) = x(q - 2d) + dp$ and $g_4(x) = x(p - 2d) + dq$, for $x \in [0, c]$. Since $q > 2d$ and $p > 2d$, the maximum is

$$g_3(d) = g_4(d) = dp + dq - 2d^2.$$

□

For any polynomial $f \in \mathbb{Z}[X]$ with appropriate degree d , there are at most $dp + dq - 2d^2$ integers which are suitable for f . We are interested in *efficient methods* to construct polynomials which are best possible in this sense. The following theorem yields a method with runtime complexity of the form $\mathcal{O}(d^{1+\epsilon})$. We will use this idea in the factorization algorithm in Section 3. Therefore, details will be explained in the proof of Theorem 3.4.

Theorem 2.9. *Let $N \in \mathbb{N}$ be semiprime with the prime factors p and q . Let $d \in \mathbb{N}$ and $b_i \in \mathbb{Z}$, $1 \leq i \leq d$. Let $f_i \in \mathcal{D}_{N, b_i}$ such that $\deg f_i = 1$ and write $f_i = l_i X + c_i$ for every i . If $\gcd(c_i, N) = 1$ for every i and also $\gcd(b_j - b_k, N) = 1$ for every choice of $j, k \in \{1, \dots, d\}$, $j \neq k$, then*

$$\nu\left(\prod_{i=1}^d f_i\right) = dp + dq - 2d^2.$$

Proof. For $1 \leq i \leq d$, consider f_i . Since $\gcd(c_i, N) = 1$, $f_i \neq 0$ as polynomial in $\mathbb{Z}_p[X]$ and in $\mathbb{Z}_q[X]$. Therefore, b_i is the only zero of f_i modulo p and modulo q .

Now consider $g := \prod_{i=1}^d f_i$. Obviously, every b_i , $1 \leq i \leq d$, is a zero of g modulo p as well as modulo q . Since $\gcd(b_j - b_k, N) = 1$ for every choice of $j, k \in \{1, \dots, d\}$, $j \neq k$, these zeros are distinct. For this reason, g has d distinct zeros modulo p and d distinct zeros modulo q . Now we apply Theorem 2.8. \square

Remark 2.10. For every polynomial f_i in the theorem above, there are $p + q - 2$ integers which are suitable for f_i . But, if we multiply all these polynomials, we do not get $d(p + q - 2)$ suitable integers for the product g . It is easy to see that there are $4 \cdot \binom{d}{2}$ integers vanishing in g . We get

$$\nu\left(\prod_{i=1}^d f_i\right) = dp + dq - 2d^2 = d(p + q - 2) - 4 \cdot \binom{d}{2}.$$

We will now prove a result to ensure the maximum possible number of suitable integers for the product of digit polynomials of degree 2, which may be compared to the result in Theorem 2.9. We will see that the b -adic digit polynomials are especially useful in this case, not only because it is easy to compute them, but also because of their uniqueness and the special way they are constructed.

Theorem 2.11. *Let $N \in \mathbb{N}$ be semiprime with prime factors p and q . Let $d \in \mathbb{N}$ and $b_i \in \mathbb{Z}$, $1 \leq i \leq d$. Let $f_i \in \mathcal{D}_{N, b_i}$ such that $\deg f_i = 2$ and write $f_i = n_{2,i}X^2 + n_{1,i}X + n_{0,i}$ for every i .*

If $\gcd(n_{2,i} \cdot b_i, N) = 1$ for every i and if for $b_{d+i} := n_{0,i} \cdot n_{2,i}^{-1} \cdot b_i^{-1} \pmod{N}$, $1 \leq i \leq d$, we have $\gcd(b_j - b_k, N) = 1$ for every choice of $j, k \in \{1, \dots, 2d\}$, $j \neq k$, then

$$\nu\left(\prod_{i=1}^d f_i\right) = 2dp + 2dq - 8d^2.$$

Proof. For $1 \leq i \leq d$, consider f_i . Since $\gcd(n_{2,i}, N) = 1$, f_i is a polynomial of degree 2 modulo p . Therefore f_i has at most two zeros modulo p . One of them is b_i . But since \mathbb{Z}_p is a field, there has to be another zero modulo p . We know from Vieta's Theorem that this zero has to be the solution of

$$n_{2,i}b_i \cdot x \equiv n_{0,i} \pmod{p}.$$

Since $b_{d+i} \equiv n_{0,i} \cdot n_{2,i}^{-1} \cdot b_i^{-1} \pmod{p}$, b_{d+i} is this zero of f_i modulo p . With similar arguments, one can also show that b_i and b_{d+i} are the zeros of f_i modulo q .

Now consider $g := \prod_{i=1}^d f_i$. Obviously, every b_i , $1 \leq i \leq 2d$ is a zero of g modulo p as well as modulo q . Since $\gcd(b_j - b_k, N) = 1$ for every choice of $j, k \in \{1, \dots, 2d\}$, $j \neq k$, these zeros are distinct. For this reason, g has $2d$ distinct zeros modulo p and $2d$ distinct zeros modulo q . Now we apply Theorem 2.8. \square

If we set $d = 1$ in the theorem above, the following statement is an immediate consequence.

Corollary 2.12. *Let $N \in \mathbb{N}$ be semiprime with prime factors p and q . Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N, b}$ with $\deg f = 2$ and $f = n_2X^2 + n_1X + n_0$. If $\gcd(n_2 \cdot b, N) = 1$ and $\gcd(N, n_2b^2 - n_0) = 1$, then $\nu(f) = 2p + 2q - 8$.*

We want to make Theorem 2.11 applicable. Hence, we have to find digit polynomials for which the condition of distinct zeros modulo the factors of N can be verified in $\mathcal{O}(d)$ steps. For the linear polynomials in Theorem 2.9 this is feasible, since we are able to choose appropriate bases, for example consecutive integers. Here, every base b_i we choose comes with a second integer b_{d+i} , which we have to control. The subsequent lemma allows to work with digit polynomials of degree 2 in practice.

Lemma 2.13. *Let $N \in \mathbb{N}$, $d \in \mathbb{N}$ and let $b_i \in \{\lceil N^{1/2}/\sqrt{2} \rceil, \dots, \lfloor N^{1/2} \rfloor\}$, $1 \leq i \leq d$, be coprime to N such that $b_{i+1} = b_i + 1$. Set $D := b_1 + \lfloor N/b_d \rfloor$.*

If $\gcd(D + z, N) = 1$ for every $z \in \{0, \dots, 2d - 2\}$ and if the b -adic digit polynomials P_{b_i} satisfy $n_{1,i} \leq n_{0,i} + 1$ for every i , then they also satisfy the conditions in Theorem 2.11.

Proof. Let $i \in \{1, \dots, d\}$ be arbitrary. It is easy to see that $n_{2,i} = 1$ for this choice of bases. Since $\gcd(b_i, N) = 1$, the first condition of Theorem 2.11 is satisfied. Now set $b_{d+i} := n_{0,i} b_i^{-1} \bmod N$. Consider the division with remainder of N with respect to b_i and write $m_i b_i + n_{0,i} = N$. We get $-m_i b_i \equiv n_{0,i} \equiv b_{d+i} b_i \bmod N$, hence $-m_i \equiv b_{d+i} \bmod N$. Next, we consider $N = (m_i - 1)(b_i + 1) + r = m_i b_i + m_i - b_i - 1 + r$ for some $r \in \mathbb{Z}$. Assume that $r \geq b_i + 1$. Then it follows that $N \geq m_i b_i + m_i$. But since $b_i \leq \lfloor N^{1/2} \rfloor$, it is easy to see that $m_i \geq b_i$. By $n_{0,i} < b_i$ we conclude

$$N \geq m_i b_i + m_i \geq m_i b_i + b_i > m_i b_i + n_{0,i} = N,$$

hence a contradiction. Now we assume that $r < 0$. Then it follows that $N < m_i b_i + m_i - b_i - 1$. But this yields that $n_{0,i} + b_i + 1 < m_i$, and by $N > b_i(n_{0,i} + b_i + 1) + n_{0,i} = b_i^2 + (n_{0,i} + 1)b_i + n_{0,i}$ we conclude $n_{1,i} > n_{0,i} + 1$, which contradicts our assumption. As a consequence, we get $0 \leq r < b_i + 1$. Because of the uniqueness of the division with remainder, there has to be $r = n_{0,i+1}$ and $m_{i+1} = m_i - 1$. Altogether we derive

$$b_{d+i+1} \equiv -m_{i+1} \equiv -m_i + 1 \equiv b_{d+i} + 1 \bmod N.$$

Now assume that there exist $j, k \in \{1, \dots, d\}$ such that $b_{d+k} \equiv b_j \bmod p$. We write $b_j = b_1 + m$ for some $m \in \{0, \dots, d - 1\}$ and, as we just have shown, we can write

$$b_{d+k} \equiv b_{2d} - l \equiv -m_d - l \equiv -\lfloor N/b_d \rfloor - l \bmod p,$$

for some $l \in \{0, \dots, d - 1\}$. It follows that $-\lfloor N/b_d \rfloor - l \equiv b_1 + m \bmod p$. Therefore, we get

$$0 \equiv b_1 + \lfloor N/b_d \rfloor + m + l \equiv D + z \bmod p,$$

for some $z \in \{0, \dots, 2d - 2\}$. But this contradicts our assumption. Hence, for every choice of $j, k \in \{1, \dots, d\}$, the integers b_{d+j} are different from the integers b_k modulo p . It is also impossible that there exist $j, k \in \{1, \dots, d\}$, $j \neq k$ with $b_{d+k} \equiv b_{d+j} \bmod p$ or with $b_k \equiv b_j \bmod p$, because this would imply $p \leq d$, which as well contradicts the assumption $\gcd(D + z, N) = 1$ for $z \in \{0, \dots, 2d - 2\}$. By similar arguments, one can show that the zeros are all distinct modulo q . \square

3 The Algorithm and its Parameters

Let $N \in \mathbb{N}$ be a composite number. Without knowledge of the factorization of N , we are able to construct a polynomial $g \in \mathbb{Z}[X]$ such that

$$1 < \gcd(g(x), N) < N,$$

for as many $x \in Z_N$ as possible. The main idea for the algorithm is to find a subset of Z_N containing at least one element which is either suitable for or vanishing in g . Let $d \in \mathbb{N}$. We work with the following parameters.

1. A set $\mathcal{B} := \{b_n \in Z_N : 1 \leq n \leq d\}$ of bases for the digit polynomials.
2. For every $b \in \mathcal{B}$, we choose exactly one $f_b \in \mathcal{D}_{N,b}$. We denote the set of all these polynomials by $\mathcal{D}(\mathcal{B})$.
3. A set $\mathcal{S} := \{s_n \in Z_N : 1 \leq n \leq d\}$, containing at least one element suitable for or vanishing in $g := \prod_{b \in \mathcal{B}} f_b$.

These three sets determine the following algorithm, and its correctness and runtime depends on finding a good choice for them.

Algorithm 3.1. *Let $N \in \mathbb{N}$ and the sets $\mathcal{B} = \{b_n \in Z_N : 1 \leq n \leq d\}$, $\mathcal{D}(\mathcal{B}) = \{f_b \in \mathcal{D}_{N,b} : b \in \mathcal{B}\}$ and $\mathcal{S} = \{s_n \in Z_N : 1 \leq n \leq d\}$ be given, where $d \in \mathbb{N}$. Set $a_1 = 1$, $a_2 = 1$ and take the following steps to factor N :*

1. *For every $b \in \mathcal{B}$, compute $f_b \in \mathcal{D}(\mathcal{B})$. Next, compute the polynomial $g := \prod_{b \in \mathcal{B}} f_b \pmod{N}$.*
2. *For every $n \in \{1, \dots, d\}$, compute $y_n := g(s_n) \pmod{N}$.*
3. *Set $j := a_1$.*
4. *If $j > d$, print 'Error A'. Otherwise compute $G_j := \gcd(y_j, N)$. If $G_j = 1$, set $a_1 = j + 1$ and go to Step 3. If $1 < G_j < N$, print G_j . We have found a nontrivial factor of N and the algorithm terminates. If $G_j = N$, go to Step 5.*
5. *Set $i := a_2$.*
6. *If $i > d$, print 'Error B'. Otherwise compute $H_i := \gcd(f_{b_i}(s_j), N)$. If $H_i = 1$ or $H_i = N$, set $a_2 = i + 1$ and go to Step 5. If $1 < H_i < N$, print H_i . We have found a nontrivial factor of N and the algorithm terminates.*

We now clarify which conditions are necessary to make the algorithm work. Finding a solution to the following problem is crucial.

Problem 3.2. *Let $N \in \mathbb{N}$ be of unknown factorization. For $d \in \mathbb{N}$, construct two disjoint sets $\{b_n : 1 \leq n \leq d\}$ and $\{s_n : 1 \leq n \leq d\}$ in Z_N with the property that, if N is composite, there must exist $i, j \in \{1, \dots, d\}$ and a prime factor p of N such that $b_i \equiv s_j \pmod{p}$.*

Example 3.3. Let $d := \lceil N^{1/4} \rceil$. Then it is easy to prove that the choice of the sets $\{-n \pmod{N} : 1 \leq n \leq d\}$ and $\{(n-1)d \pmod{N} : 1 \leq n \leq d\}$ is a solution to the problem.

A solution to Problem 3.2 could be used in an obvious way to factor natural numbers in $\mathcal{O}(d^2)$. The subsequent theorem shows how we can apply a solution to factorize much faster, using Algorithm 3.1.

Theorem 3.4. *Let N be a natural number and let $\{b_n : 1 \leq n \leq d\}$ and $\{s_n : 1 \leq n \leq d\}$ be a solution to Problem 3.2. Then Algorithm 3.1 runs in $\mathcal{O}(d^{1+\epsilon})$ with the parametrization*

$$\begin{aligned}\mathcal{B} &:= \{b_n : 1 \leq n \leq d\}, \\ \mathcal{D}(\mathcal{B}) &:= \{X - b : b \in \mathcal{B}\}, \\ \mathcal{S} &:= \{s_n : 1 \leq n \leq d\}.\end{aligned}$$

The algorithm will find a nontrivial factor of N if it is composite, and will print 'Error A' if N is prime.

Proof. Let N be composite. Since \mathcal{B} and \mathcal{S} are disjoint subsets of Z_N , we have

$$s \not\equiv b \pmod{N}$$

and therefore $f_b(s) \not\equiv 0 \pmod{N}$ for every choice of $s \in \mathcal{S}$ and $b \in \mathcal{B}$. This implies that if there is $s \in \mathcal{S}$ such that $\gcd(g(s), N) = N$, s vanishes in g and Algorithm 3.1 will find a nontrivial factor in Step 6.

It remains to show there is $n \in \{1, \dots, d\}$ with $1 < G_n \leq N$ in Step 4. Since the sets \mathcal{B} and \mathcal{S} are a solution to Problem 3.2, there is a prime factor p of N and at least one pair $(b', s') \in \mathcal{B} \times \mathcal{S}$ such that $b' \equiv s' \pmod{p}$. We get $f_{b'}(s') = s' - b' \equiv 0 \pmod{p}$, hence $1 < \gcd(g(s'), N) \leq N$.

Let N be prime. Since \mathcal{B} and \mathcal{S} are disjoint subsets of Z_N , N can not be a divisor of products of differences of their elements. There must be $G_n = 1$ for every $n \in \{1, \dots, d\}$ in Step 4, and the algorithm prints 'Error A'.

Let us discuss the runtime complexity of the algorithm. Note that the multiplication time $M(d)$ for multiplying two integers of length d can be bounded by $\mathcal{O}(d \log d \cdot \log(\log d))$.

Step 1: We have to multiply d polynomials of degree 1. There are well known methods to do this by $\mathcal{O}(M(d) \log d)$ arithmetic operations.

Step 2: Here we have to evaluate the polynomial g of degree d in d points. This can be done by $\mathcal{O}(M(d) \log d)$ arithmetic operations, using the well known methods for multipoint evaluation of polynomials.

Step 4 and Step 6: We have to compute at most d greatest common divisors in each of these steps. For this task, we employ the Euclidean Algorithm.

To summarize, the algorithm runs in $\mathcal{O}(M(d) \log d)$. That proves our claim. \square

Remark 3.5. We could choose any $f_b \in \mathcal{D}_{N,b}$ satisfying $f_b(s) \not\equiv 0 \pmod{N}$ for every $s \in \mathcal{S}$ and $b \in \mathcal{B}$. But for computational convenience, we should use $f_b = X + N - b \equiv X - b \pmod{N}$ as digit polynomial to base b . The possibility to work with a larger variety of digit polynomials seems to be more of theoretical interest and has been discussed in Section 2. For detailed information concerning the tools used in Step 1 and Step 2, we refer the reader to [GG, Ch.10], in particular, to the algorithms in 10.3 and 10.5.

Remark 3.6. (Strassen's method as special case)

Let $d := \lceil N^{1/4} \rceil$. We recall Strassen's factoring algorithm. The polynomial

$$g = (X + 1)(X + 2) \cdots (X + d)$$

is evaluated in $0, d, 2d, \dots, (d-1)d$ in order to compute all parts of $\lfloor N^{1/2} \rfloor!$ to find a factor of N . But we may also consider the method as an application of the solution presented in Example 3.3 and, therefore, as Algorithm 3.1 running with the parametrization

$$\begin{aligned} \mathcal{B} &:= \{-n \pmod{N} : 1 \leq n \leq d\}, \\ \mathcal{D}(\mathcal{B}) &:= \{X + n : 1 \leq n \leq d\}, \\ \mathcal{S} &:= \{(n-1)d \pmod{N} : 1 \leq n \leq d\}. \end{aligned}$$

This and other more or less similar solutions to Problem 3.2 yield the current deterministic complexity bound $\mathcal{O}(N^{1/4+\epsilon})$ for unconditional integer factorization. More generally, if we know that there is a prime factor smaller than $\lfloor N^{1/m} \rfloor$, which for instance has to be the case if N has at least m nontrivial factors, then it is easy to see that we have a solution for $d := \lfloor N^{\frac{1}{2m}} \rfloor$. Hence, we are able to run Algorithm 3.1 in $\mathcal{O}(N^{\frac{1}{2m}+\epsilon})$ in these cases.

4 A Computational Approach

If we want to improve the current bound for deterministic integer factorization, one way could be to find a better solution for Problem 3.2 working for a lower d , on which the runtime of the algorithm mainly depends.

Theorem 4.1. *Let $N \in \mathbb{N}$ be composite and p a prime factor of N with $p < b$ for some $b \leq N/5$. If we know a pair m, r of natural numbers with $2 \leq m < p$ such that $r = p \pmod m$, we can find a nontrivial factor of N in $\mathcal{O}(d^{1+\epsilon})$, where $d = \lceil (b/m)^{1/2} \rceil$.*

Proof. We have $p < b \leq md^2$, therefore we can write $p = mx + r$ for some $x \in \{0, 1, 2, \dots, d^2 - 1\}$. Furthermore, we write $x = i - j$ for some $i \in \{d, 2d, \dots, d^2\}$ and some $j \in \{1, 2, \dots, d\}$. We deduce $p = m(i - j) + r$, which implies $mi + r \equiv mj \pmod p$. For $n \in \mathbb{N}$, $1 \leq n \leq d$, we define

$$\begin{aligned} b_n &:= mdn + r, \\ s_n &:= mn. \end{aligned}$$

We derive $1 < m \leq s_n \leq md < md + r \leq b_n \leq md^2 + r < N$ for every $n \in \{1, \dots, d\}$, since

$$\begin{aligned} md^2 + r &= m(\lceil (b/m)^{1/2} \rceil)^2 + r < m((b/m)^{1/2} + 1)^2 + m \\ &= b + 2(bm)^{1/2} + 2m < 5b \leq N. \end{aligned}$$

As a consequence, $\{b_n : 1 \leq n \leq d\}$ and $\{s_n : 1 \leq n \leq d\}$ are disjoint subsets of Z_N and we have $b_{i/d} \equiv s_j \pmod p$. It follows that the sets are a solution to Problem 3.2 and we apply Theorem 3.4. \square

Remark 4.2. Let $N \in \mathbb{N}$, $N \geq 30$ be composite and $\lceil N^{1/6} \rceil < p < b$ a prime factor of N , where $b = \lceil N^{1/2} \rceil \leq N/5$.

1. If we know $m, r \in \mathbb{N}$ with $m \geq \lceil N^{1/10} \rceil$ and $r = p \pmod m$, we can find a nontrivial factor of N in $\mathcal{O}(N^{1/5+\epsilon})$.
2. If we know $m, r \in \mathbb{N}$ with $m \geq \lceil N^{1/6} \rceil$ and $r = p \pmod m$, we can find a nontrivial factor of N in $\mathcal{O}(N^{1/6+\epsilon})$.

If N is a composite number with more than three nontrivial divisors, we already have algorithms with runtime $\mathcal{O}(N^{1/6+\epsilon})$ to factorize N (See Remark 3.6). Therefore, we only consider the semiprime case in the following problem, which is currently unsolved. Solving it would improve the deterministic complexity bound for integer factorization to $\mathcal{O}(N^{1/6+\epsilon})$.

Problem 4.3. Let $N \in \mathbb{N}$ be semiprime with prime factors p and q and assume $p < q$. Find an algorithm with runtime $\mathcal{O}(N^{1/6+\epsilon})$ to compute a pair $(m, r) \in \mathbb{N}^2$ such that $\lceil N^{1/6} \rceil \leq m < p$ and $r \equiv p \pmod{m}$.

Now we use the idea of Theorem 4.1 to construct another solution to Problem 3.2.

Corollary 4.4. Let $N \in \mathbb{N}$ be composite and p a prime factor of N with $p \leq b$ for some $b \leq N/5$. If $r, m \in \mathbb{N}$ such that $2 \leq m < p$, $\gcd(N, m) = 1$ and $r \equiv p \pmod{m}$, then the sets

$$\begin{aligned} &\{m^{-1}r - n \pmod{N} : 1 \leq n \leq d\} \\ &\{-dn \pmod{N} : 1 \leq n \leq d\} \end{aligned}$$

are a solution to Problem 3.2, where $d = \lceil (b/m)^{1/2} \rceil$.

Proof. In the proof of Theorem 4.1 we have already shown that there are $i, j \in \{1, 2, \dots, d\}$ such that $mdi + r \equiv mj \pmod{p}$. Clearly, this implies $-di \equiv m^{-1}r - j \pmod{p}$. It remains to show that the two sets are disjoint in Z_N . Assume to the opposite that there are $x, y \in \{1, 2, \dots, d\}$ such that $-dx \equiv m^{-1}r - y \pmod{N}$. We deduce $mdx + r \equiv my \pmod{N}$. But in the proof of Theorem 4.1 we have also seen that $\{mdn + r : 1 \leq n \leq d\}$ and $\{mn : 1 \leq n \leq d\}$ are disjoint in Z_N , hence we derive a contradiction. \square

Remark 4.5. The only a priori unknown value in the sets considered in the preceding lemma is $m^{-1}r \pmod{N}$. Knowing it would immediately enable us to apply Algorithm 3.1 with $d = \lceil (b/m)^{1/2} \rceil$. Also note that $p = m\lfloor p/m \rfloor + r$ and therefore $m^{-1}r \equiv -\lfloor p/m \rfloor \pmod{p}$.

5 Characterizations for Primes

Finally, we present some characterizations of primality by digit polynomials. The major work for the following proofs is already done. Let $N \in \mathbb{N}$ be a fixed odd number. Note that it is easy to detect powers of prime numbers, which allows us to assume that N is either prime or composite with at least two different prime factors.

Theorem 5.1. Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N,b}$ with $d := \deg f$. Let d be smaller than $q := \max\{q' \in \mathbb{P} : q' \mid N\}$ and $\gcd(\text{lc } f, N) = 1$. Then the following holds:

$$N \in \mathbb{P} \Leftrightarrow \forall x \in Z_N : f^{N-1}(x) \pmod{N} \in \{0, 1\}.$$

Proof. Assume that N is prime. Then the statement immediately follows from Fermat's little Theorem.

Assume that N is a composite number. Let p be a prime factor of N such that $p \neq q$. According to Lemma 2.5 there exists $x \in \mathbb{Z}$ with $p \mid f(x)$ and $q \nmid f(x)$. Write $pj = f(x)$ for some $j \in \mathbb{Z}$. Then we get

$$f^{N-1}(x) \equiv (pj)^{N-1} \not\equiv 1 \pmod{N},$$

because otherwise there would exist $k \in \mathbb{Z}$ with $(pj)^{N-1} - 1 = pk$, hence $p \mid 1$. Since $f^{N-1}(x) \not\equiv 0 \pmod{q}$, we also derive $f^{N-1}(x) \not\equiv 0 \pmod{N}$. Therefore, we have found $x \in \mathbb{Z}$ with $f^{N-1}(x) \not\equiv 1 \pmod{N}$ and $f^{N-1}(x) \not\equiv 0 \pmod{N}$, which yields a contradiction. \square

Corollary 5.2. *Let $b \in \mathbb{Z}$ and $f \in \mathcal{D}_{N,b}$ with $d := \deg f$. Let d be smaller than $q := \max\{q' \in \mathbb{P} : q' \mid N\}$ and $\gcd(\text{lc } f, N) = 1$. Then the following holds:*

$$N \in \mathbb{P} \Leftrightarrow \forall x \in Z_N : f^{\frac{N-1}{2}}(x) \pmod{N} \in \{-1, 0, 1\}.$$

Proof. Assume that N is prime. Then the statement immediately follows from Euler's Criterion.

Assume that N is a composite number. According to Theorem 5.1 there is $x \in Z_N$ such that $f^{N-1}(x) \pmod{N}$ is neither 0 nor 1. Then $f^{\frac{N-1}{2}}(x) \pmod{N}$ is different from $-1, 0$ and 1 . Hence, this implies a contradiction. \square

Example 5.3. Let $b = N$ and let $f = X \in \mathcal{D}_{N,b}$. Then all the conditions of Theorem 5.1 and Corollary 5.2 are satisfied. We derive the well known results

$$\begin{aligned} N \in \mathbb{P} &\Leftrightarrow \forall x \in Z_N : x^{N-1} \pmod{N} \in \{0, 1\} \\ &\Leftrightarrow \forall x \in Z_N : x^{\frac{N-1}{2}} \pmod{N} \in \{-1, 0, 1\}. \end{aligned}$$

Acknowledgements

Special thanks go to Alexander Bors and to my supervisor Peter Hellekalek for their corrections and helpful suggestions.

References

- [W] S.S. Wagstaff Jr., *The Joy of Factoring*, American Math. Society, Providence, RI, 2013.
- [S] V. Strassen, *Einige Resultate über Berechnungskomplexität*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Pages 1-8, 1976/77.
- [CH] E. Costa, D. Harvey, *Faster deterministic integer factorization*, Math. Comp. 83, Pages 339-345, 2014.
- [P] C. Pomerance, *Analysis and Comparison of some Integer Factoring Algorithms*, Computational Methods in Number Theory, H.W. Lenstra Jr., and R. Tijdeman, eds., Pages 89-139, Math. Centre Amsterdam, 1982.
- [R] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics (Volume 126), Second Edition, Birkhäuser Boston, 1994.
- [CP] R. Crandall, C. Pomerance, *Prime Numbers, A Computational Perspective*, Second Edition, Springer Science+Business Media Inc., 2005.
- [GG] J. Gerhard, J. von zur Gathen, *Modern Computer Algebra*, Second Edition, Cambridge University Press, 2003.